

PATENT ABSTRACTS OF JAPAN

(11) Publication number : **07-288798**
(43) Date of publication of application : **31.10.1995**

(51)Int.Cl.

H04N	7/16
G09C	1/00
G11B	20/10
H04K	1/00
H04L	9/06
H04L	9/14
H04N	5/92
H04N	7/24

(21)Application number : 06-102205
(22)Date of filing : 15.04.1994

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : INOUE TORU

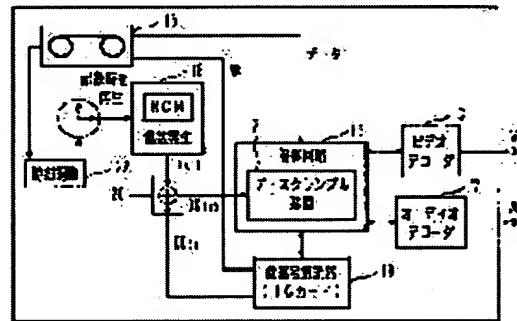
KURAHASHI SOJI
YAMADA MASAKO
YAMAZAKI TATSUO

(54) DIGITAL PICTURE RECORDING AND REPRODUCING DEVICE, REPRODUCING DEVICE, AND TV RECEPTION EQUIPMENT

(57) Abstract:

PURPOSE: To provide a television receiver having the system, where the security of cipher broadcast is more improved, or the VTR device which records ciphered data as it is and descrambles it for viewing at the time of reproducing.

CONSTITUTION: A data scrambling key is ciphered, and this data is operated with random numbers updated by clock information, and the obtained key is transmitted as a transmission key in a form of a packet. On the reception side, it is discriminated whether the header part is ciphered or not, and a data descrambling key is obtained by the same random numbers updated by a clock of the same time and an intermediate key which is obtained by deciphering the transmission key in a key deciphering device 19 like an IC card which deciphers the transmission key by a key deciphering algorithm, to descramble data, and television and ciphered data from which video data and audio data should be restored for viewing are recorded as they are, and data is restored by the data scrambling key obtained by the prescribed operation to reproduce video and audio signals.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or
application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision
of rejection]
[Date of requesting appeal against examiner's
decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

【特許請求の範囲】

【請求項1】 デジタル信号で放送するプログラム単位にプログラムヘッダーを付けそれを特定のパケットに分割してパケットヘッダーをつけパケットデータをスクランブルして伝送するデジタルTV信号であって、予め決められた鍵暗号化アルゴリズムによりデータのスクランブル鍵を暗号化し中間的な鍵を得て、時計情報によって得られた乱数と演算してデータデスクランブル鍵を暗号化して伝送された信号を受信するものであって、復号側で時計手段よりの情報により乱数を発生させる乱数発生手段、暗号化されて送信されてきたデータスクランブル鍵を解読する鍵暗号解読器、またはICカード手段により解読して得た中間的な鍵と、時計手段により発生させた乱数を演算してデータスクランブル鍵を復号する演算手段を備えてデータを復元することを特徴とするデジタルTV受信装置。

【請求項2】 回転ヘッドを用いて磁気テープにアジャス記録するデジタル録画記録再生装置であって、MPEGなどのイントラフレームと予測フレームが混在する伝送方式で、デジタル信号で送信されてきたプログラムデータをパケット形式で伝送されるビデオ信号を記録再生する録画記録再生装置であって、伝送レートR_tより記録レートR_rが大なるレートで記録する装置において、記録する際、伝送パケットのまたはプログラムのヘッダーによってデータが暗号化されているかどうか判断し、あるいはイントラなどのフレームの検出ができないことにより暗号化されていることを判別しデータが暗号化されていない場合はデータを一度復号し、その一部分（例えば特殊再生用のイントラフレームの低域成分）を抽出して伝送されてきたデータ部と受信側で抽出した一部分のデータの両方を記録レートR_rで記録し、ヘッダー部よりあるいはイントラなどのフレームが検出できないことなどにより暗号化されていると判断される場合はその暗号化されたデータをそのまま記録する記録手段を備えたことを特徴とするデジタル録画記録再生装置。

【請求項3】 請求項2で記録されたテープなどの媒体よりデータを再生する再生装置において特殊再生の時は一部抽出した成分（イントラフレームの低域成分など）により特殊再生時にも連続動画を再生するVTRにおいて、暗号化されたデータを再生するときはテープに記録された復号化鍵を所定の鍵暗号鍵読器やICカードなどにより解読して鍵を再生し、得られた鍵をもとにスクランブルされて記録されたデータをデスクランブルしてデータを再生する再生手段を備えたことを特徴とするデジタル録画再生装置。

【請求項4】 プログラムデータをパケット形式で伝送するデータ伝送信号であって、暗号化されているか否かを示す情報と、データをデ・スクランブルする鍵を暗号化して伝送し復号側で上記信号を受信してデータ鍵を解読する鍵暗号解読器またはICカードによって送信され

た暗号化鍵を復号して、受信側で時計情報による乱数と、所定の鍵復号アルゴリズムを備えた暗号解読器またはICカードにより伝送された鍵を解読した中間的な鍵とを演算した結果得られたデータスクランブル鍵によりデータを復元することを特徴とするデジタル録画再生装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はデジタル映像信号とデジタルオーディオ信号とを受信するTV装置、および、デジタル映像信号とデジタルオーディオ信号とを、斜めトラックのそれぞれ決められたエリアに記録するようなトラックフォーマットを有するデジタルビデオテープレコーダ（以下、デジタルVTRという）において、デジタル映像信号とデジタルオーディオ信号とがビットストリームで入力され、このビットストリームを記録するデジタルVTRに係わり、特にそれらの暗号化されたデータの伝送と記録と再生に関するものである。

【0002】

【従来の技術】 図6は一般的な家庭用デジタルVTRのトラック図である。図において、磁気テープには斜めトラックが構成されており、一つのトラックはデジタル映像信号を記録する映像エリアと、デジタルオーディオ信号を記録するオーディオエリアの二つのエリアに分割されている。

【0003】 このような家庭用デジタルVTRに映像およびオーディオ信号を記録するには二つの方法がある。一つは、アナログ映像信号とオーディオ信号を入力として、映像やオーディオの高能率符号化器を用いて記録する、いわゆるベースバンド記録方式である。もう一つは、デジタル伝送されたビットストリームを記録する、いわゆるトランスペアレント記録方式である。

【0004】 アメリカ合衆国で審議されているATV（Advanced Television）信号を記録するには、後者のトランスペアレント記録方式が適している。その理由は、ATV信号は既にデジタル圧縮された信号であり、高能率符号化器や復号化器が不要であることや、そのまま記録するので画質の劣化がないことなどである。

【0005】 上述のようなATV信号を記録するデジタルVTRの方式として、1993年10月26日から28日にカナダ国オタワ市で開催された“International Workshop on HDTV'93”における技術発表に、“A Recording Method of ATV data on a Consumer Digital VCR”がある。以下、この内容を従来例として述べる。

【0006】 家庭用デジタルVTRのプロトタイプの基本仕様として、SD（Standard Definition

ition) モード時、ディジタル映像信号の記録レートを 25 Mbps として、フィールド周波数が 60 Hz の場合、映像の 1 フレームを 10 トラックの映像エリアに記録するものがある。ここで、ATV 信号のデータレートを 17-18 Mbps とすると、この SD モードで ATV 信号のトランスペアレント記録が可能になる。

【0007】図 7 はデジタル VTR の通常再生時と、高速再生時におけるヘッドトレース図である。図において、各トラックは違ったアジマス角度を持つヘッドにより交互に斜め記録されている。通常再生時は、テープ送り速度が記録時と同じであるので、ヘッドは記録トラックに沿って、図 7 (a) のようにトレースすることができる。しかし、高速再生時はテープ速度が異なるためいくつかのトラックを横切ってトレースし、各同一アジマストラックの断片のみを再生することができる。図 7 (b) では 5 倍速の早送りの場合を示す。

【0008】MPEG 2 のビットストリームでは、イントラ符号化されたブロックのみが他のフレームを参照せずに独立に復号できる。もし、MPEG 2 のビットストリームが順番に各トラックに記録されているとしたら、高速再生時の再生データは固まって飛び飛びにバースト状に再生されるので、イントラ符号化されたブロックのみで画像を再構成することになる。このとき、スクリーン上では、再生されるエリアは連続ではなく、また、ブロックの断片がスクリーンに広がることになる。さらに、ビットストリームは可変長符号化されているので、スクリーンのすべてが周期的に更新される保証はなく、ある一部が長い時間更新されないこともある。

【0009】図 8 は高速再生が可能なビットストリーム記録装置のブロック図である。ここでは、各トラックの映像エリアを、全ての ATV 信号のビットストリームを記録するメインエリアと、高速再生時に画像の再構成に用いるビットストリームの重要な部分 (HP データ) を記録する複写エリアとに分ける。高速再生時は、イントラ符号化ブロックのみが有効であるので、複写エリアにこれを記録するが、さらにデータを削減するために、すべてのイントラ符号化ブロックから低域周波数成分を抜き出して、HP データとして記録する。図 8 において、101 はビットストリームの入力端子、102 はビットストリームの出力端子、103 は HP データの出力端子、104 は可変長復号器、105 はカウンタ、106 はデータ抜き取り回路、107 は EOB (End of Block) 付加回路である。

【0010】MPEG 2 のビットストリームは入力端子 101 から入力され、出力端子 102 からそのまま出力されて、メインエリアに順次記録される。一方、入力端子 101 からのビットストリームは可変長復号器 104 にも入力され、MPEG 2 のビットストリームのシンタックスが解析され、イントラ画像を検出し、カウンタ 105 にてタイミングを発生し、データ抜き取り回路 1

06 でイントラ画像のすべてのブロックの低域周波数成分を抜き出し、さらに、EOB 付加回路 107 で EOB を付加して、HP データを構成し、複写エリアに記録する。

【0011】図 9 は、図 8 の装置の再生時の動作を示す図である。通常再生時はメインエリアに記録されているすべてのビットストリームが再生され、デジタル VTR の外にある MPEG 2 復号器に送られる。HP データは捨てられる。一方、高速再生時は、複写エリアの HP データのみが集められて復号器に送られ、メインエリアのビットストリームは捨てられる。

【0012】図 10 はテープ上のメインエリアと複写エリアの例を示す図である。家庭用デジタル VTR では、各トラックの映像エリアは 135 のシンクブロックから構成されており、メインエリアは 97 シンクブロック、複写エリアは 32 シンクブロックとした。この場合、メインエリアのデータレートは約 17.46 Mbps、複写エリアは 17 回同じデータが記録されるので、約 338.8 kbps となる。

【0013】図 5 は従来の暗号化放送に用いるテレビ装置とその放送データを録画する VTR の説明図である。BS (放送衛星) テレビ放送ではコアテック方式が用いられている。(文献 1、昭和 62 年度電機通信技術審議会答申諮詢 第 18 号監修) BS の暗号方式はラインローテーションとラインパーミュテーション方式があり、ラインローテーションはテレビ画面の 1 フレームまたは 1 フィールドの各走査線内の信号を切り替える方式、ラインパーミュテーションは走査線どうしを適宜入れ換えることによりスクランブルをかける。従来 BS または CS の暗号放送は契約するとき暗号デコード装置を購入しユーザーはそれを受信機に付加する。この時ユーザーの ID 番号が登録される。使用者は使用期間の料金を支払いその間は電波によって送られてきた暗号デスクランブル鍵を自動的に解読器が解読してそれによって送信側でスクランブルされたデータをデスクランブルして視聴していた。デコード装置は TV 受像器に内蔵されているものもあった。各デコーダは向上出荷時マシン個別の ID 番号がつけられる。また CS テレビ放送では 5 つのスクランブル方式があり各種委託放送事業者はこれらの方 (①コアテック方式、②M 方式、③スカイポート方式、B-NTSC ビデオサイファー方式、⑤B-MAC 方式) を自由に選択できる(文献 2、泉 武博「ケーブルテレビ技術入門ー(基礎から応用まで)」コロナ社) には放送にスクランブルを用いる技術が詳述されている。図 5 で SM はスクランブルされたデータを復号するための鍵を解読するための鍵暗号鍵読器または解読アルゴリズムを備えた IC カードであり、この装置で送信されてきた鍵を解読してデータをデ・スクランブルする鍵を得て元のデータを復元する。復元されたデータは通常のアナログまたはデジタルの VTR にそのまま接続す

れば暗号を復号した状態で通常の番組の録画と同じように録画が可能である。

【0014】

【発明が解決しようとする課題】しかし、この方式はTV用の暗号スクランブルのデコーダーを購入した人は一度デスクランブルされたTV信号をその出力端子よりVTRにそのまま記録することができ以後無制限にダビングが可能になるという著作権上の課題があった。また、留守番録画を行いVTRで暗号放送を記録して見たいユーザーと録画はしないが、TVは暗号放送も視聴したいユーザーとを分離できないという課題があった。

【0015】本発明上記のような課題を解決するためになされたもので、暗号放送のセキュリティをより高めた方式によるデジタルTV受信装置、また、暗号データを暗号されたまま記録し、再生時に暗号をデ・スクランブルして試聴するデジタル録画記録再生装置及びデジタル録画再生装置を提供することを目的とする。

【0016】

【課題を解決するための手段】本発明の請求項1に係るデジタルTV受信装置は、復号側で時計手段よりの情報により送信側に同期して同じ手順で乱数を発生させる乱数発生手段、送信してきた暗号化されたデータスクランブル鍵を解読する暗号解読器、またはICカード手段により解読して得た中間的な鍵と時計情報により発生させた乱数を演算してデータスクランブル鍵を復号する演算手段を備えてデータを復元するものである。

【0017】本発明の請求項2に係るデジタル録画記録再生装置は、伝送パケットのまたはプログラムのヘッダーによってデータが暗号化されているかどうか判断する手段、あるいはイントラなどのフレームの検出ができないことにより暗号化されていることを判別する手段、データが暗号化されていない場合はデータを一度復号し、その一部分（例えば特殊再生用のイントラフレームの低域成分）を抽出して伝送してきたデータ部と受信側で抽出した一部分のデータの両方を記録レートR_rで記録し、ヘッダー部より暗号化されていると判断される場合はその暗号化されたデータをそのまま記録する記録手段を備えたものである。

【0018】本発明の請求項3に係るデジタル録画再生装置は、暗号化されたデータを再生するときはテープに記録された復号化鍵を所定の鍵暗号鍵読器やICカードなどにより解読して鍵を再生し、得られた鍵をもとにスクランブルされて記録されたデータをデスクランブルしてデータを再生するデ・スクランブル手段を備えたものである。

【0019】本発明の請求項4に係るデジタル録画記録再生装置は、時計情報により作成された乱数と、所定の鍵暗号アルゴリズムで暗号化した鍵との演算結果を伝送し、受信側で時計手段よりの情報により乱数を発生する算数発生手段、所定の鍵復号アルゴリズムを備えた暗

号解読器またはICカード、により伝送された鍵を解読した中間的な鍵を時計よりの乱数と演算する演算手段、その結果得られたデータスクランブル鍵によりデータを復元するデ・スクランブル手段を備えたものである。

【0020】

【作用】本発明は送信してきた暗号化データをVTRに暗号化されたデータのまま記録し正当なユーザーが正当な手続きで記録再生することができる暗号解読デコーダまたはICカードを備えているのでTVとVTRを独立の別々の契約で放送を試聴することができVTRの契約者は留守番録画などにより暗号スクランブルデータのまま一旦録画し、後日暗号解読器またはICカードにより暗号化鍵を解読してデータのスクランブル鍵を復号して試聴することが出来る。

【0021】本発明の請求項1に係るデジタルTV受信装置においては、時計情報より定期的に更新される乱数情報発生し、予め決められた鍵暗号アルゴリズム実行手段とにより演算をする演算手段を備えてデータをスクランブル、デ・スクランブルする鍵を暗号化する作用がある。

【0022】本発明の請求項2に係るデジタル録画記録再生装置においては、ヘッダー情報によって暗号化されているかどうかを判別し暗号化されていないときはデータを復号し、その一部を抽出して記録レートR_rで記録しヘッダー情報により暗号化されていないと判断した場合はそのデータを暗号化されたままで記録する作用がある。

【0023】本発明の請求項3に係るデジタル録画再生装置においては、暗号化されたデータを再生するときテープに記録された伝送鍵をICカードなどの鍵暗号鍵読手段により解読してデータのデ・スクランブル鍵を取り出す作用があり、暗号化されて記録されたデータからデータをデ・スクランブルして元のビデオ、オーディオデータを復元する作用がある。

【0024】本発明の請求項4に係るデジタル録画再生装置においては、記録された時刻情報より再生した記録時の時計情報を得る作用あるいは記録された時刻情報より調整して記録時の時刻情報を再生する作用があり、ICカードなどの鍵暗号解読手段と併せ用いて演算する作用がある。

【0025】

【実施例】

実施例1. 図1は本発明に係るTV受信装置を示すブロック図である。図において、1はデジタルテレビ信号入力端子、2はモ뎀およびヘッダーデコード手段、3は時計機能手段、4は乱数発生手段、5は制御回路によるコントロール手段、6はビデオ信号デコード手段、7はオーディオ信号デコード手段、8は鍵暗号解読器、またはICカード、9は演算手段1、10はスクランブル手段、11はビデオ信号出力端子、12はオーディオ

信号出力端子である。

【0026】図2は伝送されたデータからデ・スクランブルする鍵を復号するシーケンスを説明する図である。端子1より入力された受信デジタルTV信号は2のモデム手段によりデジタルパターンに復調される。データは放送プログラム毎にプログラムヘッダーが付加された後、パケット単位に分割される。各パケットはパケットヘッダーが先頭に付加される。こうして伝送されたベースバンドのデジタル信号が再生され、プログラムヘッダーおよびパケットヘッダーの解読が行われる。図で制御回路5は受信データよりデータ鍵を運搬する送信鍵TK(i)を受信データより抽出して暗号解読器8へ送り、中間的な鍵出力KK(i)を得る。KK(i)は演算装置19へ入力される。一方、時計情報より発生された乱数r(i)が演算装置19へ入力され演算結果としてDK(i)を得る。時計情報より発生された乱数r

(i)とはスクランブル、デ・スクランブルに用いられる乱数は例えば同一PN(pseudo noise)シーケンスを発生するシフトレジスターを送信、受信でデータに法2加算して送信し、受信側で送信データに対応させて同一のPNシーケンスパターンを法2加算して元の情報を得る。この場合、スクランブルの初期値が鍵となる。このDK(i)がデータを直接スクランブルした時の鍵に対応する復号鍵であるのでデ・スクランブル装置10へ送ってデータを復元し、ビデオ部分はビデオデコーダ6へ、オーディオ部分はオーディオデコーダ7へ送り、各々デコードしてビデオ出力およびオーディオ出力を得る。

【0027】パケットヘッダーには各パケットが暗号化されているかどうかを示すフラグがかかっており、プログラムのヘッダーはパケットの後に続いてかかれ、暗号化されたデータの場合は特定のいくつかのフィールドに繰り返してデ・スクランブルするための鍵情報がかかれる。

【0028】図2ではプログラムパケットが大きいときはプログラムを適当なパケットづつ区切って伝送パケットとプログラムパケットの中間的な適当な大きさの、いわばスクランブルユニット単位のストリームにし、その単位で鍵を配送する。プログラムパケットが小さいときは鍵の更新は以下のようにする。図2で一番上のシーケンスは送信鍵が送られてくる状態を示したもので各伝送パケットのヘッダーに奇数番目か偶数番目かの区別を示すフラグがあり、それに基づいて常に2つの鍵が送られてくる。その様子がいちばん上の送信鍵シーケンスである。図の点線は時刻iの鍵データはTK(i)を受信してから時間TAの間にデータ鍵を解読してDK(i)なる鍵を得る。一方、時計情報からの乱数r(i)を得て、それを所定の演算(例えば、いちばん簡単な例では法2加算)を行い、DK(i)を例えれば、

$$DK(i) = r(i) + KK(i)$$

より得る。但し、ここで+記号は法2加算を示し、EXOR(Exclusive OR; 排他的論理和)で実現される。得られた鍵DK(i)は送信側でデータをスクランブルした鍵に同じになるので、これを例えれば、データに法2加算してデータを取り出す。

$$I(i) = DATA(i) + DK(i)$$

ここで、DATA(i)は送られてきたプログラムデータである。このようにしてビデオとオーディオのデジタル情報を復元したのちビデオ信号はビデオデコーダ6でオーディオ信号はオーディオデコーダ7で各々復号して各々ビデオ出力、オーディオ出力を端子V、Aより出力する。

【0029】ここで、時計情報による乱数とは図2の送信鍵シーケンスTK(i)より得られた中間的な復号鍵系列KK(i)と同じ更新時間間隔で乱数r(i)を発生するもので送信、受信で例えば同一のROMにかかれた乱数データを正確な時計を送信、受信で同期させて中間的な復号鍵系列KK(i)と同じ更新時間期間で乱数を発生させる。正確な時計情報で同一ROMなどに記録されている乱数データを更新して乱数を発生する。演算装置9は送信、受信で同じ演算アルゴリズムを持ち発生させた乱数r(i)を復号鍵KK(i)を入力して一定の演算を行い、データ復元用デ・スクランブル鍵DK(i)を得る。

$$DK(i) = F(KK(i), r(i); i)$$

で与えられる。F(・)はKK(i)とr(i)の関数となる。このようにしてデータ復元鍵DK(i)を得てスクランブル手段10でデータを復元しビデオ信号はビデオデコーダ、オーディオ信号はオーディオデコーダで元のビデオ信号、オーディオ信号を得て各々端子A、Vより出力する。

【0030】実施例2. 図3は本発明によるVTRの記録時の動作を説明する図であり、図4は本発明によるVTRの再生時の動作を説明する図である。図において、13はデジタルTV信号入力端子、14はモデムおよびヘッダーデコーダー、15は記録を行うカセットテープ、16は制御回路、17は記録時刻を示す時計機能である。

【0031】図4で18は時計情報より乱数を発生させる乱数発生手段、19はICカードなどによる鍵暗号解読手段、20は復号鍵DK(i)を演算して出力する演算手段II、21はデータを復元するためのデ・スクランブル手段、22はカセットテープよりの再生時刻情報より送信時刻を再現してそれにより時計機能を入力させて送信時の欄数を発生させる時刻調整機能である。

【0032】まず、記録動作について説明する。端子13より入力されたデジタルTV信号は14のモデムでベースバンド信号になりヘッダーデコーダーで暗号化されているかどうかなどの制御情報や時刻、番組情報、契約や課金情報、個別(ペイパービューか、契約種別、フ

ラットフィー情報など) 情報などを取り出す。プログラムまたは伝送パケットのヘッダーによってデータが暗号化されているかどうか判別出来ない時はイントラなどのフレーム検出ができないことにより暗号化されていると判断する。この時、暗号化データをそのままカセットに記録すると同時に記録時の時刻情報をカセットに同時に記録しておく。個別情報には全有料番組が視聴できるフラットフィー (Flat-free) 契約、例えば映画番組、スポーツ番組のみが試聴できるティア (Tier) 契約、試聴した分だけ料金を支払うペイペービュー (Pay-per-View) がある。ヘッダー部にはプログラムの開始時刻や終了時刻など各種時刻情報が入っているのでそれらを記録する。カセットテープに番組の録画と同時に記録する、又書いてない場合はVTRが内蔵している正確な時計により記録時の時刻情報をカセットに記録しておく。

【0033】再生時には暗号化データが制御回路のなかのスクランブル手段へ入力されてデータが復元される。ここで用いられるデータ復元鍵DK (i) の再生について述べる。送信時の鍵TK (i) は送信時の鍵暗号アルゴリズムに対応した鍵解読アルゴリズムを内蔵したICカードなどの鍵暗号鍵読手段によって中間的な解読鍵K (i) が得られる。一方、カセットテープより記録時の時刻情報が再現されその情報をもとにVTRの時計機能を記録時の時刻に同期させる。乱数発生手段18は再生された記録時の時計により得られた時刻情報より送信時のスクランブルデータに対応した乱数r (i) を発生し演算手段II20へ送る。演算手段II20では入力されたr (i) とKK (i) より所定の演算を行いデータをデ・スクランブルする鍵DK (i) を得る。

【0034】このようにして、データ用のデ・スクランブル鍵が復号できたのでデ・スクランブル手段によってデータを復元し、ビデオデコーダ6、オーディオデコーダ7で元のビデオ、オーディオ信号を得る。なお、以上は鍵暗号化鍵、鍵復号化鍵が同じ鍵を用いる慣用暗号系を用いる例で説明したが鍵暗号化鍵と鍵復号化鍵が異なる公開鍵を用いる方式でも同一の効果がえられることはあきらかである。

【0035】公開鍵暗号系は暗号化鍵rと復号化鍵sが異なっており復号化鍵は秘密に保持されるが暗号化鍵rは公開されている。代表的な公開鍵暗号であるRSA暗号の場合、平文aに対して暗号文bを、

$$b = a^r \pmod{n}$$

より計算して求める。nは大きな2つの素数p、qの積で与えられる。解読側ではこれをs乗する。

$$b^s = a^{rs} = a \pmod{p} = a \pmod{q}$$

であるので、

$$\therefore b^s = a \pmod{n}$$

となり平文aが復元される。RSA暗号はこのように法nの演算で実行される。従って公開鍵暗号を用いても暗

号化鍵を公開するしないは本発明の基本的な部分でないのでデータスクランブル鍵DK (i) を暗号化する鍵r (i) で行い、ICカード等による鍵解読器による鍵復号演算をRSA暗号の復号化技術s (i) を用いれば慣用暗号とあとは同様に扱えばよい。

【0036】

【発明の効果】本発明は送信されてきた暗号化データをVTRに暗号化されたデータのまま記録し正当なユーザーが正当な手続きで記録再生することができる鍵暗号解読デコーダまたはICカードを備えているのでTVとVTRを独立の別々の契約で放送を試聴することができVTRの契約者は留守番録画などにより暗号スクランブルデータのまま一旦録画し、後日鍵暗号解読器またはICカードにより暗号化鍵を解読してデータのスクランブル鍵を復号して試聴することが出来る。

【0037】本発明の請求項1に係るデジタルTV受信装置によれば、時計情報より定期的に更新される乱数情報発生手段と、予め決められた鍵暗号アルゴリズム実行手段とにより演算をする演算手段を備えてデータをスクランブル、デ・スクランブルする鍵を暗号化しているのでよりセキュリティ効果の高いテレビ受像器が実現できる効果がある。

【0038】本発明の請求項2に係るデジタル録画記録再生装置によれば、ヘッダー情報によって暗号化されているかどうかを判別し暗号化されていないときはデータを復号し、その一部を抽出して記録レートRrで記録し、ヘッダー情報により暗号化されていないと判断した場合はそのデータを暗号化されたままで記録する記録手段を備えているので、暗号化されたデータでもVTRに記録再生する効果がある。

【0039】本発明の請求項3に係るデジタル録画再生装置によれば、暗号化されたデータを再生するときデータに記録された伝送鍵をICカードなどの鍵暗号鍵読手段により解読してデータのデ・スクランブル鍵を取り出す機能を有しているので暗号化されて記録されたデータから再生されたデータをデ・スクランブルして元のビデオ、オーディオデータを復元できる効果がある。

【0040】本発明の請求項4に係るデジタル録画再生装置によれば、記録された時刻情報より再生した記録時の時計情報を得る手段あるいは記録された時刻情報より調整して記録時の時刻情報を再生する手段を備えているのでICカードなどの鍵暗号解読手段と併せ用いて演算することによりデ・スクランブル鍵を得ることができそれによって記録された暗号化データをデ・スクランブルしてビデオ、オーディオ信号を復元する効果がある。

【図面の簡単な説明】

【図1】 本発明に係るTV受信装置を示すブロック図である。

【図2】 伝送されたデータからデ・スクランブルの鍵を復号するシーケンスを説明する図である。

【図3】 本発明のVTRの記録時の動作を説明する図である。

【図4】 本発明のVTRの再生時の動作を説明する図である。

【図5】 従来のスクランブル放送を受信するテレビとVTRの説明図である。

【図6】 一般的な家庭用デジタルVTRのトラック図である。

【図7】 デジタルVTRの通常再生時と高速再生時におけるヘッドトレース図である。

【図8】 高速再生が可能なビットストリーム記録装置を示すブロック図である。

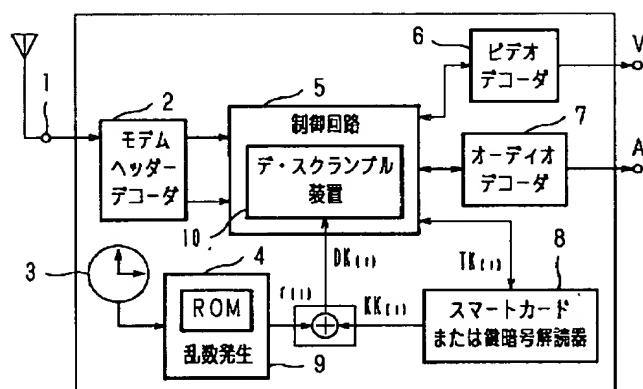
【図9】 図8の装置の再生時の動作を示す図である。

【図10】 テープ上のメインエリアと複写エリアの例を示す図である。

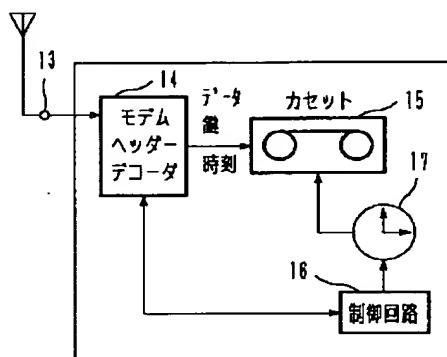
【符号の説明】

2 ビデオおよびヘッダーデコーダー、3 時計あるいは時刻再生手段、4 亂数発生手段、5 制御回路、6 ビデオデコーダー、7 オーディオデコーダー、8 I Cカードまたは手段、9 演算手段I、10 デ・スクランブル手段、14 VTR内のモデムおよびヘッダーデコーダー、15 デジタルVTRカセット、16 制御回路、17 時計あるいは時刻再生機能手段、18 亂数発生器、19 暗号解読手段、20 演算手段I、21 デ・スクランブラー、22 時刻調整手段。

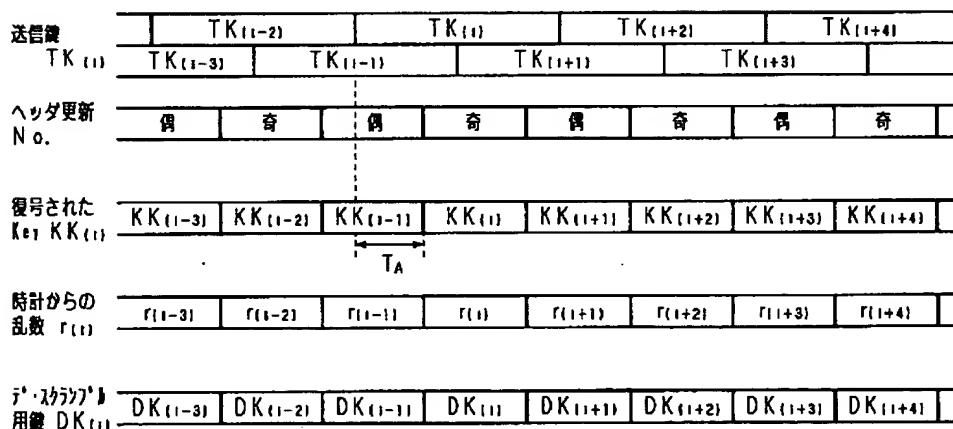
【図1】



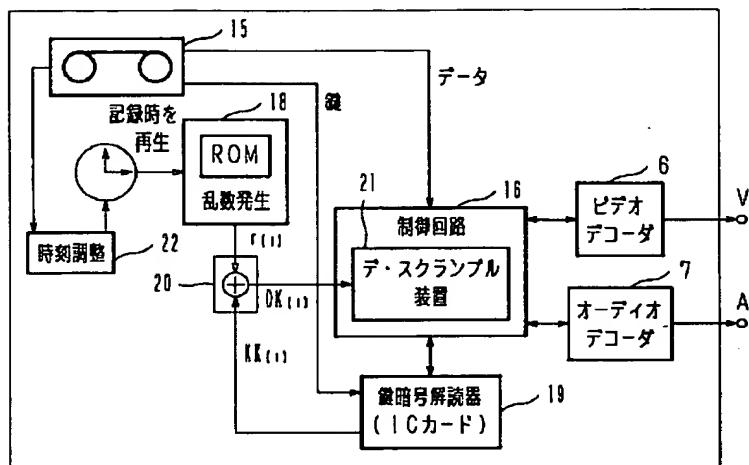
【図3】



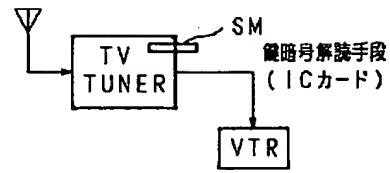
【図2】



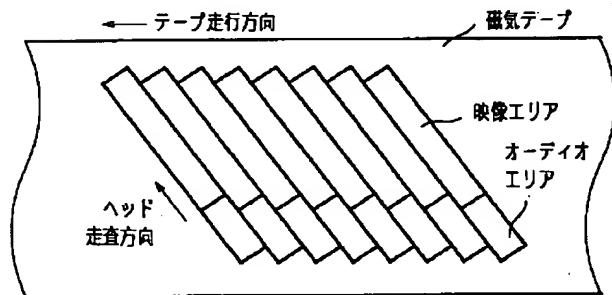
【図4】



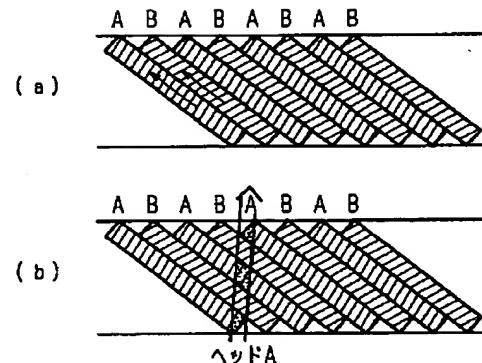
【図5】



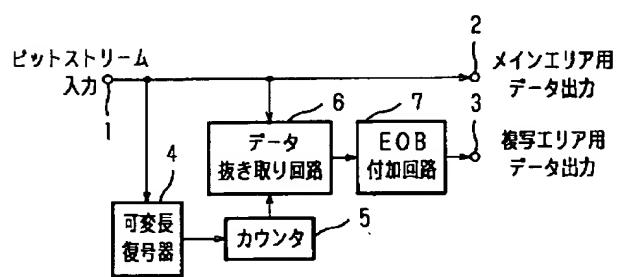
【図6】



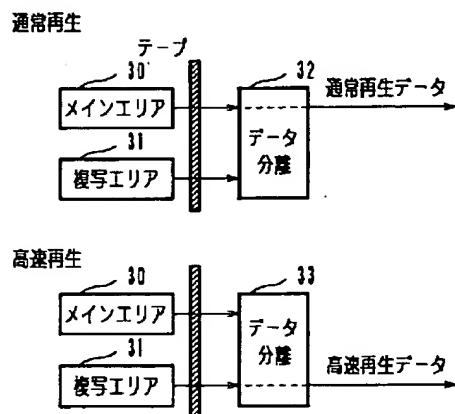
【図7】



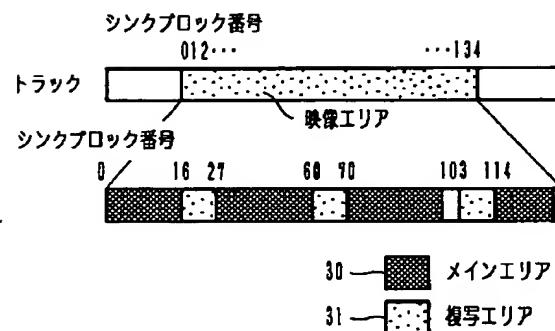
【図8】



【図9】



【図10】



フロントページの続き

(51) Int.Cl. ⁶	識別記号	府内整理番号	F I	技術表示箇所
H 0 4 K	1/00	Z		
H 0 4 L	9/06			
	9/14			
H 0 4 N	5/92			
	7/24			
			H 0 4 N 7/13	Z

(72)発明者 山崎 辰男

長岡京市馬場岡所1番地 三菱電機株式会
社映像システム開発研究所内

光ディスク投入リスト(追加入力依頼分)

No.	受付番号	依頼日	ディスクNO	ディスク	備考
1	318505875KR1		21A		登録
2	318507045KR1		11A		登録
3	318704770IN1		23A		登録
4	318704816IN1		18A		登録
5	318705555IN1		19A		登録
6	318801848US1		21A		登録
7	319000512EP1		2B		登録
8	319001484EP1	2001/1/31			登録
9	319101430EP1		2B		登録
10	348600045KR1		7A		登録
11	348801428US1		15B		登録
12	349300175EP1	2001/6/13			放棄
13	349300406US1	2001/1/31			登録
14	349500163US1	2001/1/31			登録
15	349501192US1		1B		放棄
16	349601105US1		1B		放棄
17	349701159KR1	2001/6/13			放棄
18	349701537US1	2001/6/13			放棄
19	349705296US1	2001/6/13			放棄
20	349800140US1	2001/6/13			放棄
21	349905093US1	2001/6/13			放棄

光ディスク投入リスト(追加入力依頼分)

